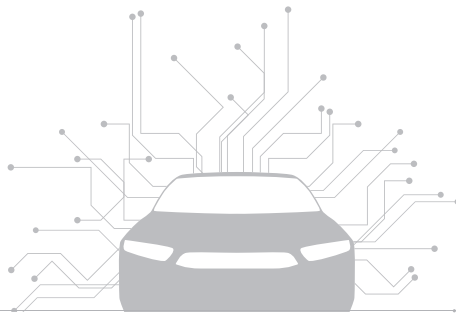
스마트카의 사이버보안 기술



심상규 펜타시큐리티시스템(주) IoT융합보안연구소 소장

1. 머리말

우리는, 그동안 우리가 일상에서 봐왔던 자동차의 개념을 넘어서 새로운 자동차로 진화하는 시대를 살고 있다. 현재의 자동차도 단순한 기계 부품들의 조합이라 이해할 수 있는 수준을 오래전에 넘어 섰다. 자동차에 필요한 소프트웨어의 분량이 1억 라인에 달하여, F-35 전투기나 보잉 787 여객기에 필요한 소프트웨어의 분량보다 4~6배 이상 많은 것으로 분석되고 있다[1]. 자동차의 진화를 이끄는 가장 핵심의 요인 중 하나는 V2X 통신으로 지칭되는 외부 통신 기능이다. 자동차는 엄청난 분량의 소프트웨어와 외부 통신을 바탕으로 점점 똑똑하고 심지어는 자율적으로 움직이는 자동차로 거듭나고 있다.

이러한 자동차의 변화상을 두고 많은 이들은 보안에 대한 걱정을 하고 있다. 기존 IT에서도 해킹을 포함한 보안 사고로 인해 많은 피해가 발생하고 있다. 기존 IT에서의 해킹은 금전적 피해를 주더라도 인명에 직접 피해를 주지는 않는 반면, 자동차의 해킹은 인명 사고로 직접 이어질 수 있어 큰 걱정이 아닐 수 없다.

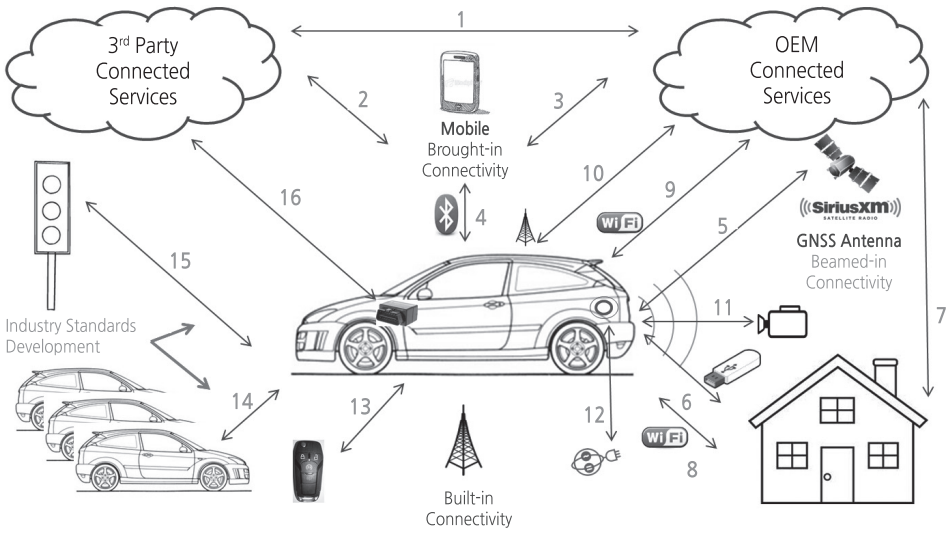
본고는 자동차를 둘러싼 보안 위협을 살펴보고, 보안 기술의 적용을 위한 방향을 모색해 보고자 한다.

2. 외부 통신을 중심으로 한 자동차의 변화

2.1 확장 자동차(Extended Vehicles)

외부 통신을 중심으로 자동차의 변화상을 가장 잘 정의한 것은 ISO/TC22/SC31/WG6에서 표준화를 진행하고 있는 ISO20077과 ISO20078[2]이다. [그림 1]의 14번과 15번의 외부 통신은 V2V(Vehicle-to-Vehicle)인 차량 간 통신과 V2I(Vehicle-to-Infrastructure)인 차량과 인프라 간 통신이다. 차량과 제조사 클라우드 간 통신인 9번과 10번은 차량 제조사의 미래 사업을 위해 중요한 서비스로 인식되고 있다. 그 외에도 제조사 클라우드를 매개로 차량과 가정의 Home IoT와 연결하는 시나리오(7번)는 차량의 연결을 Home IoT로 확대할 수 있다는 점에서 매우 중요하다. 2016년 1월에 폭스바겐이 CES 전시회에서 LG전자의 냉장고와 연결하는 것을 발표한 바 있고, 최근에 가전사들이 냉장고를 첨단화하고 'Family Hub'로 설명하는 것과 맞닿아 있다.

우리가 더욱 눈여겨볼 점 중 하나는 16번의 시



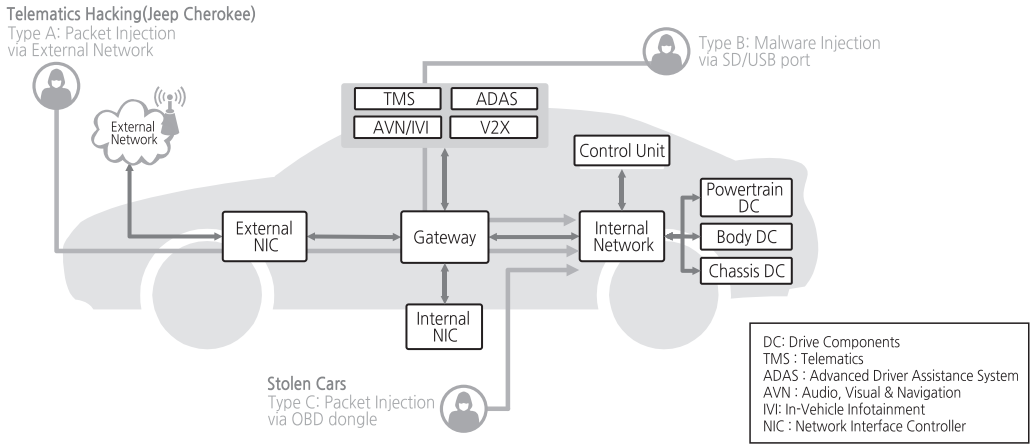
[그림 1] ISO 20077이 정의하는 서비스 범위[2]

나리오이다. 자동차가 제조사 클라우드 이외의 다른 클라우드에 연결이 된다는 것은, 제조사가 선택하지 않은 소프트웨어가 자동차 내부에 탑재된다는 것을 의미한다. 이 소프트웨어는 제조사가 아니라, 사용자가 선택하게 될 것은 분명하다. 우리는 이러한 변화를 피처폰이 스마트폰으로 변화하는 과정에서 이미 체험한 바 있다. 피처폰도 인터넷 연결을 제공하고 다양한 소프트웨어들이 탑재되었지만, 스마트폰은 그보다 더 다양한 소프트웨어를 통해 다양한 인터넷 서비스를 폭넓게 사용할 수 있게 되었다. 피처폰의 소프트웨어는 제조 과정에서 제조사에 의해 탑재되었지만, 스마트폰의 소프트웨어 중 대부분은 구매 후 사용자의 선택에 의해 설치되며 이들 소프트웨어는 대개 제공사의 클라우드와 연결된다. 현재의 자동차는 피처폰과 마찬가지로 모든 소프트웨어가 제조 공정에서 탑재되지만, 향후의 자동차는 사용자의 선택에 의해서 설치되는 소프트웨어들이 생겨나게 될 것이고, 자동차는 스마트폰처럼 철저하게 개인화된 기기로 진화하게 될 것이다.

2.2 자동차의 해킹의 유형

최근 10여 년 동안 자동차의 해킹과 관련하여 다양한 연구와 사례들이 발표되었다. [그림 2]의 유형 C는, 자동차의 OBD 단자에 동글(dongle)을 연결하고 동글과 연결된 컴퓨터를 사용하여 자동차에 멀웨어나 공격 패킷을 주입하는 방법이다. 자동차의 OBD 단자에 설치하는 동글은 스마트폰 어플과 함께 판매되어, 운전자에게 차량의 상태를 잘 알 수 있도록 해주는 데에 사용되기도 한다. 유형 B는 유형 C보다 진화한 방법으로서, 자동차의 멀티미디어 서비스를 위해 탑재되어 있는 USB나 SD 단자를 활용하여 멀웨어나 공격 패킷을 주입하는 방법이다.

유형 B나 C는 공격자가 자동차에 물리적으로 접촉해야 하는 것에 반해서, 유형 A는 공격자가 자동차에 전혀 접촉하지 않더라도 공격이 가능하다는 점이 큰 차이이다. 이 공격의 대표적인 사례는 2015년 7월의 Jeep Cherokee 모델을 해킹한 것이다. 이로 인해, 제조사는 140만 대에 달하는 차량을 회수하는데 이르렀고, 자동차의 소프트웨어 패치를 위해 OTA(Over-The-Air)에 대한 필요성이 크게 주목받



[그림 2] 자동차 해킹의 유형

는 계기가 되기도 했다. 차량이 이동통신을 사용하는 경우라 하더라도, OpenBTS[3] 기술에 기반하여 개발된 사설 이동통신 기지국을 활용한다면 차량에 탑재된 이동통신 단말이 사설 기지국과 통신하도록 만듦으로써 공격을 하는 방법도 충분히 가능하다.

3. 자동차 보안에 대한 연구 사례

3.1 자동차의 보안 위협 분류

유럽 ENISA는 2016년 12월 '스마트카의 보안과 복원력' 보고서에서 자동차에 보안 위협을 야기하는 원인을 다음 8가지로 분류하였다[4].

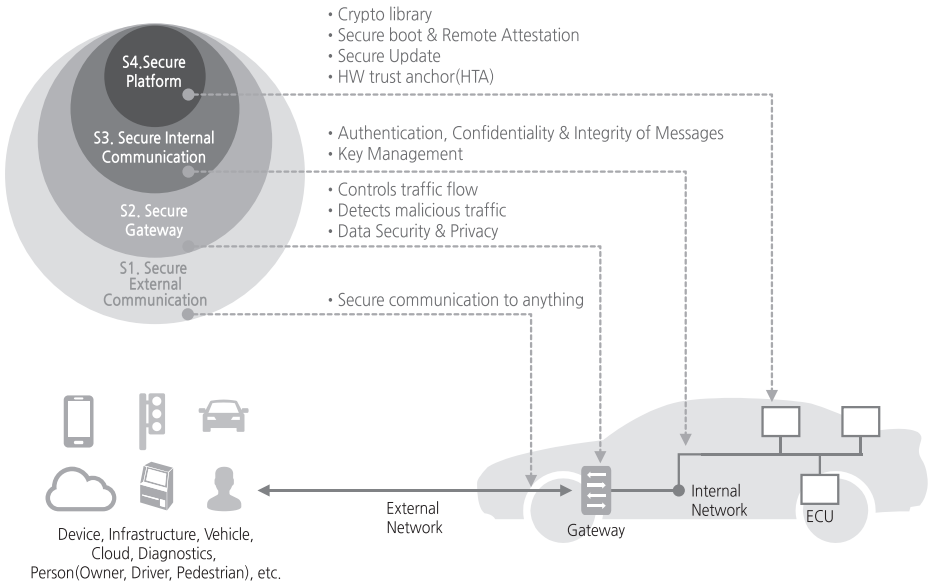
- 손실 및 분실(Damage/Loss)
- 오류 및 오동작(Failures/Malfunctions)
- 사고(Unintentional Damages/Accidental)
- 오남용(Nefarious Activity/Abuse)
- 통신 두절(Network Outage)
- 도감청 및 탈취(Eavesdropping/Interception/Hijacking)
- 물리적 위협(Physical Threats)
- 지능형 지속 공격(APT, Advanced Persistent Threats)

도감청 및 탈취는 해커들의 적극적인 행위에 의해 발생하는 것이지만, 분실, 오동작, 사고 등에 의해서 발생하는 보안 위협도 중요하게 인식하고 있다. 사용하던 스마트폰의 분실이나 고장, 혹은 고장으로 인한 수리의 과정에서 스마트폰에 저장되어 있던 중요 정보들이 유실되어 사회적 문제가 되었던 사례들을 상기해본다면 스마트카에서도 유사한 보안 위협이 존재할 수 있다는 것을 유추할 수 있다. 또한, 사용자의 오남용 행위에 의해서도 자동차의 안전(safety)을 해치고 보안을 위협할 수 있는 사례들도 발생 가능하다. 스마트폰의 루팅이나 탈옥 등에 의한 개조로 인해 보안 강도가 저하되고 해킹에 노출되는 것과 유사한 경우로 이해할 수 있다.

3.2 자동차 보안을 위한 방안

미국 고속도로안전원은 '현대 자동차를 위한 보안 우수 사례' 보고서를 통해, 자동차의 보안 대책으로 다음과 같은 기술들을 제시하고 있다[5].

- Limit Developer/Debugging Access in Production Devices



[그림 3] 외부 통신과 내부 통신의 보안

- Control Keys
- Control Vehicle Maintenance Diagnostic Access
- Control Access to Firmware
- Limit Ability to Modify Firmware
- Control Proliferation of Network Ports, Protocols and Services
- Use Segmentation and Isolation Techniques in Vehicle Architecture Design
- Control Internal Vehicle Communications
- Log Events
- Control Communication to Back-End Servers
- Control Wireless Interfaces

대략적으로 요약해보자면, ①개발자를 비롯하여 차량 내 소프트웨어나 펌웨어의 접근 및 수정을 제한, ②통신 포트, 프로토콜, 서비스 등의 무분별한 채용을 지양, ③외부 통신 혹은 내부 통신에서의 보안 적용, ④전장 아키텍처 상에서 핵심 부품에 대한 분리 보안 적용이다. 이 기술들을 적용한다면 자동차의 보안을 확보할 수 있겠지만, 어떻게 보안을 적용할 것인가에 대한 고민은 제조사와 개발사의 몫으로 남는다. 다음 장에서는 자동차의 외부 통신과 외부 통신에서의 보안을 어떻게 적용할 수 있을 것인가를 중점적으로 살펴보고자 한다.

4. 자동차 보안 적용

자동차에서 보안 문제가 대두되는 것은 자동차에 유선 혹은 무선 통신의 연결성이 생겼기 때문이다. 자동차는 통신을 통해 외부와 데이터를 송수신하고, 수신한 데이터는 자동차의 내부 네트워크를 통해 자동차에 탑재된 전장부품까지 전달된다. 이 과정 전체에 대해서 보안을 적용하기 위해서는 [그림 3]과 같은 계층적 보안의 접근이 필요하다.

4.1 외부 통신의 보안

외부 통신의 보안은 인증과 암호화로 정의할 수

있다. 데이터를 주고받는 주체들, 다시 말해, 자동차와 외부 주체 간의 인증이 먼저 이루어지고, 기밀성을 요구하는 데이터에 대해서는 암호화 통신을 적용하는 것이다. 자동차와 외부 주체들 간의 인증은 정부 주도의 접근 방식과 제조사 중심의 접근 방식에 차이가 있다. 정부는 자동차가 달리는 도로를 중심으로 인프라를 구축하는 입장에서 접근하기 때문에 다양한 제조사의 자동차들과 도로가 인증을 하고 데이터를 송수신하기 위해서 국가 표준을 제정할 필요가 있다. 그러나, 제조사는 자사의 자동차와 자사의 클라우드, 특정 기기들과 연결한 서비스를 타제조사에 대비하여 경쟁력 있게 제공하여야 하므로 타 제조사와 호환되는 표준적인 기술을 토대로 서비스를 구축할 필요성이 적다. 정부 주도의 V2X 보안에는 IEEE1609.2 표준 기술이 해외 선진국들을 비롯한 국내에서 사용되고 있으며, 이 표준 기술은 타원곡선 암호시스템과 자동차 환경에 특화된 공개키 인증서를 토대로 구성되어 있다.

4.2 게이트웨이에서의 보안

게이트웨이에서의 보안으로서 외부 통신을 통해 유입되는 통신 트래픽으로부터 자동차 전장 전체를 보호하기 위한 보안이라 할 수 있다. 게이트웨이 계층에서는 ①외부로부터 유입된 공격 트래픽의 탐지, ②내부 네트워크로의 연결 경로 제어, ③내부 데이터의 보호와 개인정보 보호를 담당하게 된다. 이를 이해하기 위해 기존 IT 환경에서 기업의 네트워크를 살펴보자. 기업의 네트워크는 컴퓨터와 서버로 구성된 사설 네트워크이고, 차량 내부의 네트워크는 전자제어장치(ECU)들로 구성된 사설 네트워크라 할 수 있다. 기업 네트워크와 인터넷의 연결 접점에 침입탐지시스템을 설치하고 외부 방화벽과 내부 방화벽을 설치하여 비무장지대(DMZ)를 설정하는 것이 일반적이다. 이와 마찬가지로, 자동차의 내부 네트워크를 보호하기 위해서는 자동차와 외부 네트워크의 접점에서 공격 트래픽을 탐지하고, 내부 네트워크로 진입하는 트래픽에 대해서 연결 경로를 제어해야 한다.

차량이 서비스 서버 등 외부 개체로부터 정보를 수신하여 차량 내부의 전자제어장치에서 활용하는 경우도 있겠지만, 그와 반대로 차량 내부의 데이터를 모아서 온라인 서버나 클라우드로 전송하고 데이터를 수신한 서버는 수신한 데이터를 가공해서 서비스의 부가가치를 높이기 위해 활용하는 경우도 존재한다. 이의 경우, 차량의 데이터를 내부에서 수집하고 안전하게 저장 · 관리하였다가 외부 서버로 전송할 때에는 개인정보의 유출이 없도록 보호해주는 기술이 필요하다.

4.3 내부 네트워크의 보안

차량의 내부 네트워크는 전자제어장치 간의 네트워크로 정의할 수 있다. 전자제어장치들은 서로의 기능을 조율하기 위해 많은 양의 데이터를 주고받는다. 이때, 공격 트래픽이 유입되거나 위변조가 발생한다면 전자제어장치의 오동작을 유발할 수 있고, 나아가서는 자동차 전체의 안전을 해칠 수 있다. 내부 네트워크의 통신에서 필요한 보안은 일반 IT 환경의 네트워크 보안과 동일하게, 인증과 암호화의 적용이라 할 수 있다. 차량의 외부 통신의 보안과는 달리, 대칭키암호알고리즘들이 더욱 효율적일 수 있다. 차량 내의 전자제어장치들은 저성능의 CPU로 대량의 데이터를 고속으로 처리해야 하는 경우가 많기 때문이다.

내부 네트워크의 암호화 통신을 위해서는 전자제어장치들을 위한 키관리가 필수불가결이다. 차량 내부 네트워크의 전자제어장치를 위해 외부 네트워크의 키관리 서버가 연결될 수는 없으므로, 차량 내부에서 키관리를 담당할 수 있는 부품, 혹은 장치가 필요하게 된다. 차량 내부의 키관리 장치는 제조사가 수립한 키관리 정책에 의해 전자제어장치들이

사용할 키를 생성, 발급, 갱신, 폐지, 삭제하는 등의 키 전주기(lifecycle)를 관리하여야 한다.

4.4 전자제어장치를 위한 보안

전자제어장치를 하나의 작은 컴퓨터로 이해하여 보안을 위해서는 ①시큐어부트(Secure Boot), ②원격 검증(Remote Attestation)과 ③펌웨어나 소프트웨어의 안전한 갱신이다. 전자제어장치에 전원이 공급되고 부팅을 시작한 이후, 설계나 개발 과정을 통해 의도된 상태에 부합하도록 펌웨어나 소프트웨어 등이 정상적으로 구동되었는지를 자가 검증하는 것이 시큐어부트이다. 시큐어부트에 의해 자가 검증되었다 하더라도 제3자에게 정상적인 동작 상태임을 검증 가능하게 해주는 기술이 원격 검증이다. 더불어, OTA 기술에 기반하여 펌웨어나 소프트웨어를 안전하게 갱신하는 것도 이 계층에서 필요한 보안 기술이다.

5. 맺음말

자동차를 바라보는 관점은, 자동차를 독립된 하나의 기기로 바라보는 관점과 자동차 내부에 존재하는 전자제어장치 간의 사설 네트워크의 집합체로 바라보는 관점이 존재한다. 이 두 관점에서 적절하게 보안을 적용하는 것이 중요하다. 첫 번째 관점에서 자동차와 외부 개체 간의 인증에 관해서는 표준 기술이 존재하지만, 두 번째 관점에서 그 외의 보안 기술에 대해서는 표준 기술이 존재하지 않고 부품사나 제조사의 독자적인 기술을 적용하여야 한다.

자동차가 커넥티드카가 되고 스마트카가 되는 등의 진화를 거듭하는 한편에는 보안에 대한 걱정이 늘 함께 존재한다. 보안 측면에서 안전한 자동차를 만들기 위해서는 자동차의 설계 단계에서부터 보안을 충분히 고려한 개발, 이른바 'Security by Design'이 이루어져야 할 것이다.

[참고문헌]

[1] Codebases: Millions of lines of code, http://www.informationisbeautiful.net/visualizations/million-lines-of-code, 2015.09.

[2] ISO/TC22/SC31, https://www.iso.org/committee/5383568.html

[3] OpenBTS, http://openbts.org

[4] 'Cyber Security and Resilience of smart cars', ENISA, 2016.12. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[5] 'Cybersecurity Best Practices for Modern Vehicles', US NHTSA, 2016.10.

[주요 용어 풀이]

- V2X(Vehicle-to-Everything, 차량·사물 통신): 유무선 통신을 통해 차량과 외부 기기 혹은 서비스와의 연결을 일컫는 총칭.
- OBD(On-Board Diagnostics): 자동차의 점검과 유지관리를 위해 사용되는 직렬통신 규격.
- OTA(Over-The-Air): 무선통신을 통해 기기의 펌웨어나 소프트웨어를 갱신 또는 설치하는 기술.
- ECU(Electronic Control Unit, 전자제어장치): 자동차의 부품들을 제어하는 전자 장치.